

Appl. No. 09/429,174

Response Dated October 14, 2003

Reply to Office Action Dated July 16, 2003

Amendments to the Specification

Please replace the paragraph beginning at page 5, line 11, which starts with the phrase "The pre-boot security controller is preferably" with the following amended paragraph.

a' The pre-boot security controller is preferably an IC which includes a [nonvolatile] non-volatile password memory that stores at least one user password. The pre-boot security controller also includes a password input circuit for receiving a password that is to be compared with any user passwords recorded in the password memory. If the pre-boot security controller is in a security operating mode, a digital logic circuit included in the pre-boot security controller compares the password received by the password input circuit with any user passwords recorded in the password memory. If the password received by the password input circuit matches a user passwords recorded in the password memory, an output circuit included in the pre-boot security controller, which is coupled to the digital logic circuit, transmits an output signal to the power subsystem that enables the power subsystem to energize the digital computer's operation.

Appl. No. 09/429,174

Response Dated October 14, 2003

Reply to Office Action Dated July 16, 2003

Please replace the paragraph beginning at page 9, line 11, which starts with the phrase "When the DC/DC converter 32 first supplies VCC" with the following amended paragraph.

a²

When the DC/DC converter 32 first supplies VCC electrical power to the pre-boot security controller 42, a signal supplied to the pre-boot security controller 42 via a RST# signal-line 54 is negated and a password has been previously recorded into a 512 byte [nonvolatile] non-volatile, electronically rewritable flash memory 56, the pre-boot security controller 42 enters a security operating mode. When the pre-boot security controller 42 is in the security operating mode, an output control 62, included in the pre-boot security controller 42, transmits signals to the DC/DC converter 32 via a OUT_PWR# signal-line 64 and an OUT_SUS# signal-line 66 that inhibit the DC/DC converter 32 from energizing operation of the digital computer 22, and other portions of the electronic device 20 not illustrated in FIG. 1. Thus, while the signals present on the OUT_PWR# signal-line 64 and OUT_SUS# signal-line 66 are asserted, the electronic device 20, except for the pre-boot security controller 42, the clock control 48 and a portion of the DC/DC

Appl. No. 09/429,174

Response Dated October 14, 2003

Reply to Office Action Dated July 16, 2003

a²
converter 32, is inoperable. Moreover, to apprise a user of the electronic device 20 that the pre-boot security controller 42 is in the security operating mode, the output control 62 transmits a signal on a LED signal-line 68 which illuminates a LED included in a status output subsystem 72 illustrated in FIG. 1.

Please replace the paragraph beginning at page 12, line 12, which starts with the phrase "A mode selection circuit 92" with the following amended paragraph.

a³
A mode selection circuit 92 included in the pre-boot security controller 42 may receive input signals via a SUSPEND# signal-line 94 and via a PWROFF# signal-line 96. When the electronic device 20 is unlocked, the state machine 52 responds to assertion of signals received via the keypad bus 84 and/or the PWROFF# signal-line 96 by negating the signals present on the OUT_PWR# signal-line 64 and on the OUT_SUS# signal-line 66. Negation of these two signals turns-off electrical power to the electronic device 20 except for the pre-boot security controller 42, the clock control 48 and a portion of the DC/DC converter 32. Such an event may occur when the user turns the

Appl. No. 09/429,174

Response Dated October 14, 2003

Reply to Office Action Dated July 16, 2003

a³
electronic device 20 off. However, such an event may also occur if a computer program executed by the digital computer 22 causes the electronic device 20 to enter a power conserving operating mode in which the current operating state of the electronic device 20 is stored into a [nonvolatile] non-volatile memory such as a hard disk, and in which operation of the digital computer 22 and other portions of the electronic device 20 are suspended.

[Please replace the paragraph beginning at page 13, line 5, which starts with the phrase "Upon suspending operation of the electronic device 20," with the following amended paragraph.]

Upon suspending operation of the electronic device 20, the pre-boot security controller 42 correspondingly enters its suspend operating mode. If the pre-boot security controller 42 is in the suspend operating mode, toggling a signal supplied to the mode selection circuit 92 via an ARM# signal-line 98 transitions the pre-boot security controller 42 from the suspend operating mode to its security operating mode. If the pre-boot security controller 42 enters the security operating mode from the

Appl. No. 09/429,174

Response Dated October 14, 2003

Reply to Office Action Dated July 16, 2003

a³
suspend operating mode, as mentioned previously restoring the electronic device 20 to full operation requires that the user enter a password that is recorded in the flash memory 56. However, if the state machine 52 remains in the suspend operating mode following entry of a valid password and does not enter the [suspend] security operating mode, then the electronic device 20 may be restored to full operation without the user re-entering a password.

Please replace the paragraph beginning at page 15, line 8, which starts with the phrase "A SMBus interface 122 included in the pre-boot security controller 42" with the following amended paragraph.

a⁴
A SMBus interface 122 included in the pre-boot security controller 42 provides a second way by which the user and supervisor passwords may be recorded into the flash memory 56. As depicted in FIG. 1, a SMBus 124 interconnects the SMBus interface 122 of the pre-boot security controller 42 with a SMBus host 126 included in the electronic device 20. Usually the electronic device 20 provides the SMBus host 126 in one of two different

Appl. No. 09/429,174
Response Dated October 14, 2003
Reply to Office Action Dated July 16, 2003

a⁴
ways. One way in which the electronic device 20 provides the SMBus host 126 is by including a system controller IC that has the SMBus host 126, e.g. an Intel Corporation 82371SB IC identified as "Southbridge." [A description of Intel's Southbridge IC, that is hereby incorporated by reference, can be obtained at the following Internet address.

<http://developer.intel.com/design/intarch/embdmod1.html>

Another way in which the pre-boot security controller 42 can provide the SMBus host 126 is by including an embedded controller, a keyboard controller or a power management controller IC that has the SMBus host 126. Additional, more detailed information about the SMBus specifications and protocol is provided by:

System Management Bus Specification, Revision 1.1,

© 1996, 1997, 1998, Benchmarq Microelectronics Ind., Duracell Inc., Energizer Power Systems, Intel Corporation, Linear Technology Corporation, Maxim Integrated Products, Mitsubishi Electric Corporation, National Semiconductor Corporation, Toshiba Battery Co., Varta Batterie AG, December 11, 1998; and

Appl. No. 09/429,174

Response Dated October 14, 2003

Reply to Office Action Dated July 16, 2003

System Management Bus BIOS Interface Specification,

*Revision 1.0, © 1996, Benchmark Microelectron-
ics Ind., Duracell Inc., Energizer Power
Systems, Intel Corporation, Linear Technology
Corporation, Maxim Integrated Products,
Mitsubishi Electric Corporation, National
Semiconductor Corporation, Toshiba Battery
Co., Varta Batterie AG, February 15, 1995.*

The publications listed above are hereby incorporated by
reference as though fully set forth here.
